PATENT ABSTRACTS OF JAPAN

(11)Publication number : 06-141192
(43)Date of publication of application : 20.05.1994

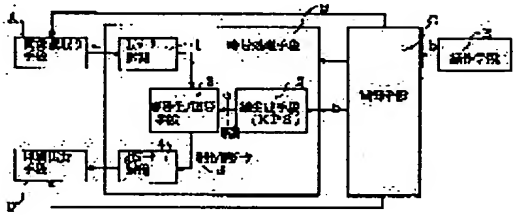
(51)Int.Cl. H04N 1/44
G09C 5/00

(21)Application number : 04-327141
(22)Date of filing : 26.10.1992

(71)Applicant : PANPUKIN HOUSE:KK
(72)Inventor : IMAI HIDEKI

(54) COPYING MACHINE WITH CIPHER FUNCTION

(57)Abstract:
PURPOSE: To provide the copying machine with cipher function prepares enciphered documents and drawings, which can be deciphered by only a specific person, without preliminary arrangement and cipher key delivery.
CONSTITUTION: This cipher key generating system consists of a picture read means A which reads information of documents, drawings, or the like, an enciphering/deciphering means 3 which enciphers or deciphers information, a key generating means 2 which prepares a cipher key used for enciphering/ deciphering, a control means C for various control, a print output means D which prints out picture information, and an operation means E for operation. This system uses a key sharing type cipher (KPS) theory, and the identifier of a specific entiry or names specifying a name specifying a document, a drawing or the like is inputted to prepares a cipher key.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

先行資料

(19)日本国特許庁（JP）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平6－141192

(43)公開日　平成6年(1994)5月20日

(51)Int.Cl.⁵	識別記号	庁内整理番号	FI	技術表示箇所
H04N 1/44		2109－5C		
G09C 5/00		8837－5L		

審査請求　未請求　請求項の数3(全 5 頁)

(21)出願番号　特願平4－327141

(22)出願日　平成4年(1992)10月26日

(71)出願人　393009356
株式会社パンプキンハウス
神奈川県厚木市飯山1620番地の1　アメニテイヒル本厚木717

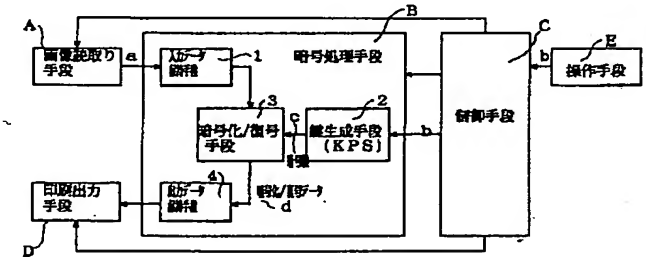
(72)発明者　今井　秀樹
神奈川県横浜市南区六ツ川3－76－3

(54)【発明の名称】　暗号機能付き複写機

(57)【要約】　(修正有)

【目的】　前もって打ち合せや暗号鍵の配送を行わずに特定の人だけが復号できる暗号化書類、図面を作成する暗号機能付き複写機を提供する。

【構成】　書類、図面等の情報を読取る画像読取り手段、情報の暗号化又は復号を行う暗号化／復号手段、暗号化／復号に用いられる暗号鍵を生成する鍵生成手段、各種の制御を行う制御手段、画像情報を印刷出力する印刷出力手段、そして操作を行う為の操作手段より成る。この暗号鍵生成システムは鍵共有方式暗号システム（KPS）理論を用い、特定のエンティティの識別子、又は書類、図面等を特定する名前を入力して暗号鍵を生成することを特徴とする。



1

【特許請求の範囲】

【請求項１】　紙などの媒体に描写された画像情報及び／またはそれを符号化した情報を入力し、これを暗号化した状態で印刷し、又印刷された暗号画像を読みとって復号し元の画像に戻して印刷及び／またはデイスプレイに表示を行う暗号機能付き複写機において、各エンテイテイ（人、装置等）が、半固定的に用いるもので任意に定められる公開の識別子を有し、センタ（管理者）だけが持つ特別なアルゴリズム（データ）と、エンテイテイの識別子に一方向性でランダムな単射を行う識別子変換を施したものとを演算させて、エンテイテイに固有な秘密アルゴリズム（データ）を生成してエンテイテイがこれを保持し、暗号化／復号を行う際に任意エンテイテイの識別子または任意の名前等を識別子として識別子変換を施したものと自分の秘密アルゴリズムとを演算させることにより、打合せや第三者による配送を必要とせずに、自分と任意のエンテイテイ又は任意の名前等に固有の鍵（暗号鍵）を生成し、この鍵を用いて、前記画像情報の暗号化／復号を行うことを特徴とする暗号機能付き複写機。

【請求項２】　前記秘密アルゴリズムに識別子を入力して暗号鍵を生成する鍵生成手段と暗号化／復号手段を内蔵した外部装置を接続し、外部装置内で暗号鍵の生成及び画像情報の暗号化または暗号画像の復号を行うことを特徴とする請求項１の暗号機能付き複写機。

【請求項３】　前記秘密アルゴリズムに識別子を入力して暗号鍵を生成する鍵生成手段を内蔵した外部装置を接続し、外部装置内で生成させた暗号鍵を用いて暗号化／復号を行う暗号化／復号手段を内蔵することを特徴とする請求項１の暗号機能付き複写機。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、暗号機能付き複写機に関する。

【０００２】

【従来技術】書類、図面などの情報を複写機で複写を行うようにして入力し、暗号化した状態で印刷して保管することによって内容の漏洩を防ぎ、必要なときに復号して元に戻すことを可能とした装置が提案された。

【０００３】

【発明が解決しようとする問題点】特定の人だけが復号できる暗号化書類、図面を作成する場合、暗号鍵の打合せが必要であり、さらにその鍵を安全に保管する為の管理が必要となる。又、多くの異なる書類、図面を暗号化する時に、同一の暗号鍵を用いたのでは安全性に問題があり、異なる暗号鍵を用いるにはその決定と管理が大変である。さらに、印刷された暗号書類、図面を、暗号化したのとは別の場所にある装置で復号する場合、暗号鍵の打ち合せや配送が必要である。

【０００４】

2

【課題を解決する為の手段】本発明は、任意のエンテイテイの識別子を入力するだけで暗号鍵を生成する鍵共有方式暗号システム（以下、ＫＰＳという）の理論を用い、特定のエンテイテイの識別子、又は書類、図面等を特定する名前を入力して暗号鍵を生成し、暗号化を行うことにより、暗号鍵の打ち合せと保管の管理が不要で、且つ特定のエンテイテイだけが復号を行うことができると共に書類図面の名前を入力するだけで暗号処理を行うことが可能な暗号機能付き複写機を実現した。

【０００５】

【実施例】図１は、本発明による暗号機能付き複写機の一実施例を示した図である。本暗号機能付き複写機（以下、本機と称する）は、画像読取り手段Ａ、暗号処理手段Ｂ、制御手段Ｃ、印刷出力手段Ｄ、及びユーザが本機を制御する為の操作手段Ｅから構成される。暗号処理手段Ｂは、入力データ保持手段１、鍵生成手段２、暗号化／復号手段３、出力データ保持手段４で構成される。

【０００６】ここで、打合せや第三者による暗号鍵（鍵）の配送を必要とせずに、自分と任意のエンテイテイに固有の鍵を生成するＫＰＳについて説明する。エンテイテイとは、一般に通信に於ける当事者となる人や装置などを示すが、ここでは人間、文書図面、装置、及びそれらを構成要素とするシステムを含む。

【０００７】エンテイテイｉが、半固定的に用いるもので任意に定められる公開の識別子を有し、これを識別子Ｙｉとし、これに一方向性でランダムな単射を行う識別子変換Ｆを施したものをＺｉ（数式１）とする。センタだけが持つ特別なアルゴリズム（データ）Ｇと、前記Ｚｉとを演算させて、エンテイテイｉに固有な秘密アルゴリズム（データ）Ｘｉ（数式２）を生成する。

【数１】

$$Zi = F(Yi)$$

【数２】

$$Xi = G(Zi)$$

エンテイテイｉは、自分の秘密アルゴリズムＸｉにエンテイテイｊの識別子Ｙｊを識別子変換したものＺｊまたは任意の名前等を識別子Ｙｘとして識別子変換したものＺｘを入力し、演算させて（数式３、４）、エンテイテイｊとの共通な暗号鍵ｋｉｊまたは任意の名前に固有の暗号鍵ｋｉｘを生成させることができる。またエンテイテイｊの秘密アルゴリズムＸｊに、エンテイテイｉの識別子Ｙｉを識別子変換したＺｉを入力して演算し（数式５）、鍵ｋｊｉを生成させることができ、これが前記ｋｉｊに等しい（数式６）ので、エンテイテイｉが暗号鍵ｋｉｊで暗号化した内容は、エンテイテイｊに復号させることができる。暗号鍵ｋｉｘを用いて暗号化した内容は、秘密アルゴリズムＸｉを持つエンテイテイｉ以外では復号できない。

【数３】

$$kij = Xi(Zj)$$

【数４】

$$kix = Xi\ (Zx)$$

【数５】

$$kji = Xj\ (Zi)$$

【数６】

$$kij = kji = k$$

ＫＰＳの理論的な詳細ついては、文献１から文献５等に記述されている。

【０００８】識別子を入力して暗号鍵を生成する鍵生成手段２は、図２のように構成される。前述の識別子変換Ｆを含む識別子変換手段５、前記秘密アルゴリズムを格納する秘密アルゴリズム格納手段６、及びそれらから暗号鍵を生成する演算手段７で構成される。

【０００９】図３は、本発明請求項２の一実施例を示す図である。図中Ａ、Ｃ、Ｄ、Ｅ及び１から４は図１に同じである。本装置は、インタフェースＰを通じて鍵生成手段２と暗号化／復号手段３を内蔵した外部装置Ｑと接続し、鍵生成及び暗号処理を外部装置Ｑで行わせる。操作手段Ｅから入力されたエンテイテイの識別子ｂが、制御手段Ｃからインタフェースを経て外部装置Ｑ内の鍵生成手段２へ送られ、暗号鍵ｃが生成されて暗号化／復号手段３に送られる。画像読取り手段Ａで読取られた画像情報ａは入力データ保持手段１を経て制御手段Ｃへ送られ、インタフェースＰを通じて外部装置Ｑの暗号化／復号手段３へ送られ、暗号鍵ｃを用いて暗号化／復号が実行される。暗号／復号データは制御手段Ｃにより、出力データ保持手段４を経て印刷出力手段Ｄに送られ、用紙上に印刷出力される。

【００１０】図４は、本発明請求項３の一実施例を示す図である。図中Ａ、Ｂ、Ｃ、Ｄ、Ｅ及び１から４は図１に同じである。本装置は、暗号処理手段Ｂを有し、インタフェースＰを通じて鍵生成手段２を内蔵した外部装置Ｑと接続され、外部装置Ｑの鍵生成手段２で生成した暗号鍵ｃを用いて暗号処理手段Ｂで暗号化／復号をおこなう。操作手段Ｅから入力されたエンテイテイの識別子ｂが、制御手段Ｃからインタフェースを経て外部装置Ｑ内の鍵生成手段２へ送られ、暗号鍵ｃが生成され、インタフェースＰを経て制御手段Ｃから暗号処理手段Ｂ内の暗号化／復号手段３に送られる。画像読取り手段Ａで読取られた画像情報ａは入力データ保持手段１を経て暗号化／復号手段３へ送られ、ここで暗号鍵ｃを用いて暗号化／復号が実行され、出力データ保持手段４を経て印刷出力手段Ｄで用紙上に印刷出力される。

【発明の効果】本発明は、特定の相手だけが復号できる暗号化書類、図面を作成する場合に、暗号鍵の打合せや管理を不要とする。さらに、暗号化する書類、図面の名前などを識別子として入力し、それらに固有の暗号鍵を生成させて暗号化／復号を行うことにより、暗号処理を簡便にすると共に安全性を高めることができる。さらに、暗号鍵の生成、又は暗号鍵の生成と暗号処理手段を外部装置で行うことにより、暗号化して印刷された書類、図面を、暗号化した装置とは別の場所にある装置で復号させることができると共に、複数のエンテイテイが独自に鍵生成手段または鍵生成手段と暗号化／復号手段とを内蔵した外部装置を所有することにより、一台の暗号機能付き複写機をそれぞれのエンテイテイが各自で鍵を管理して使用することを可能とした。

【図面の簡単な説明】

【図１】本発明請求項１の一実施例とその動作を説明する図である。

【図２】鍵生成手段の一実施例とその動作を説明する図である。

【図３】本発明請求項２の一実施例とその動作を説明する図である。

【図４】本発明請求項３の一実施例とその動作を説明する図である。

【符号の説明】

Ａ	画像読取り手段
Ｂ	暗号処理手段
Ｃ	制御手段
Ｄ	印刷出力手段
Ｅ	操作手段
Ｐ	インタフェース
Ｑ	外部装置
ａ	画像情報
ｂ	識別子
ｃ	暗号鍵
ｄ	暗号化／復号データ
１	入力データ保持手段
２	鍵生成手段
３	暗号化／復号手段
４	出力データ保持手段
５	識別子変換手段
６	秘密アルゴリズム格納手段
７	演算手段

【文献１】松本勉、今井秀樹、”第３の鍵共有方式”、１９８６年暗号と情報セキュリテイワークショップ講演論文集、１９８６年８月。

【文献２】松本勉、今井秀樹、”簡便な暗号鍵共有方式”、電気通信学会誌ＩＴ８６－５４、Ｐ－２９～３４、１９８６年９月。

【文献３】松本勉、今井秀樹、”キー　プレデイストリビューション」システムの一方式”（”ＫＥＹ　ＰＲＥ　ＤＩＳＴＲＩＢＵＳＩＯＮ　ＳＹＳＴＥＭ　ＢＡＳＥＤ　ＯＮ　ＬＩＮＥＡＲ　ＡＬＧＥＢＲＡ”）、第９回情報理論とその応用シンポジウム、ＳＩＴＡ’８６，１９８６年１０月。

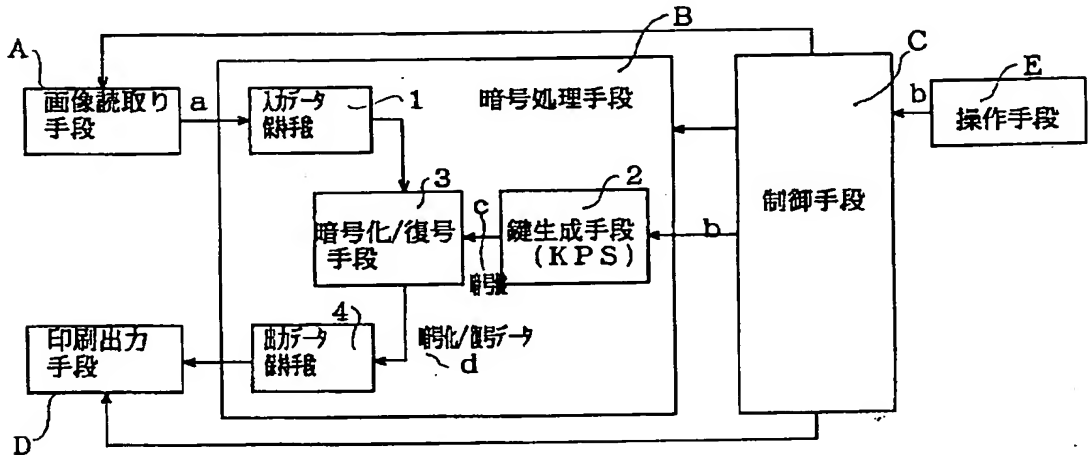
【文献４】松本勉、今井秀樹、”アプライング　ザ　キー　プレデイストリビューション　システム　トウ　エレクトリニク　メイル　アンド　シグネチュア”，情報

5
理論とその応用シンポジウム、ＳＩＴＡ’８７，１９８７年１１月。（Ｔｓｕｔｏｍｕ ＭＡＴＳＵＭＯＴＯ ａｎｄ，Ｈｉｄｅｋｉ ＩＭＡＩ，”Ａｐｐｌｙｉｎｇ ｔｈｅ Ｐｒｅｄｉｓｔｒｉｂｕｔｉｏｎ Ｓｙｓｔｅｍｔｏ Ｅｌｅｃｔｒｏｎｉｃ Ｍａｉｌｓ ａｎｄ Ｓｉｇｎａｔｕｒｅｓ”，ＳＩＴＡ’８７，ＮＯＶ．，１９８７．）

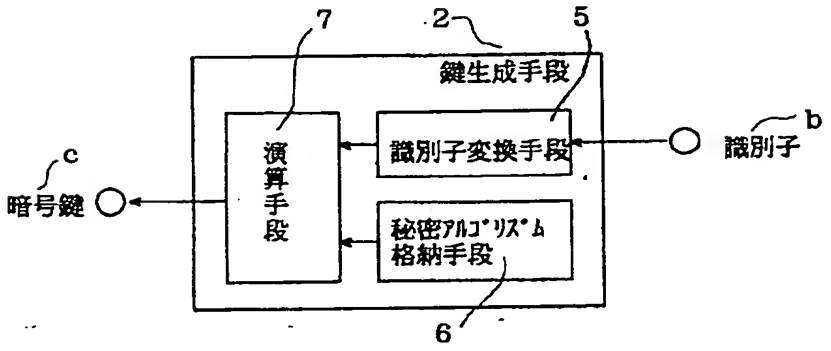
【文献５】松本勉、今井秀樹、”パフォーマンス オブ リニア スキーム フォア ザ キー プレデイスト

6
リビューション システム”、ＩＥＩＣＥ情報セキュリテイ技術報告、５月２０日号、１９８９年。（Ｔｓｕｔｏｍｕ ＭＡＴＳＵＭＯＴＯ ａｎｄ，Ｈｉｄｅｋｉ ＩＭＡＩ，”Ｐｅｒｆｏｒｍａｎｃｅ ｏｆ ｌｉｎｅａｒ ｓｅｈｅｍｅｓ ｆｏｒｔｈｅ Ｋｅｙ Ｐｒｅｄｉｓｔｒｉｂｕｔｉｏｎ Ｓｙｓｔｅｍ”，ＩＥＩＣＥ Ｔｅｅｈｎｉｅａｌ ｒｅｐｏｒｔ ｏｎ Ｉｎｆｏｒｍａｔｉｏｎ Ｓｅｃｕｒｉｔｙ，Ｍａｙ ２０，１９８８．）

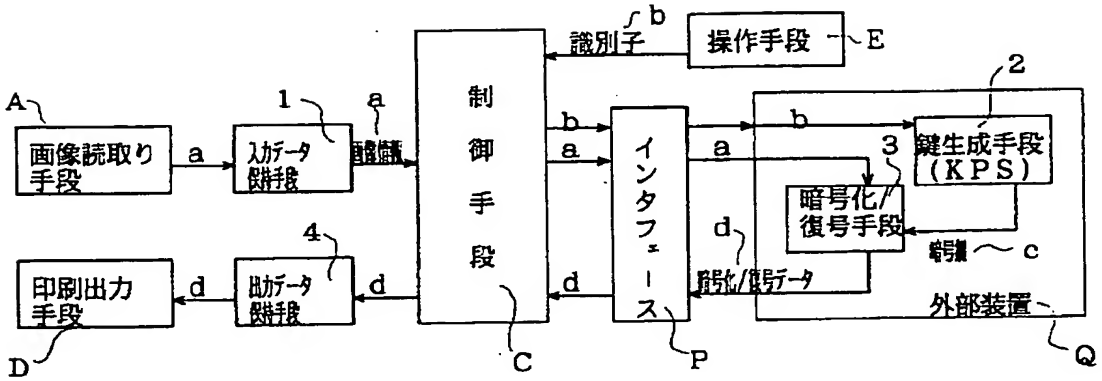
【図１】



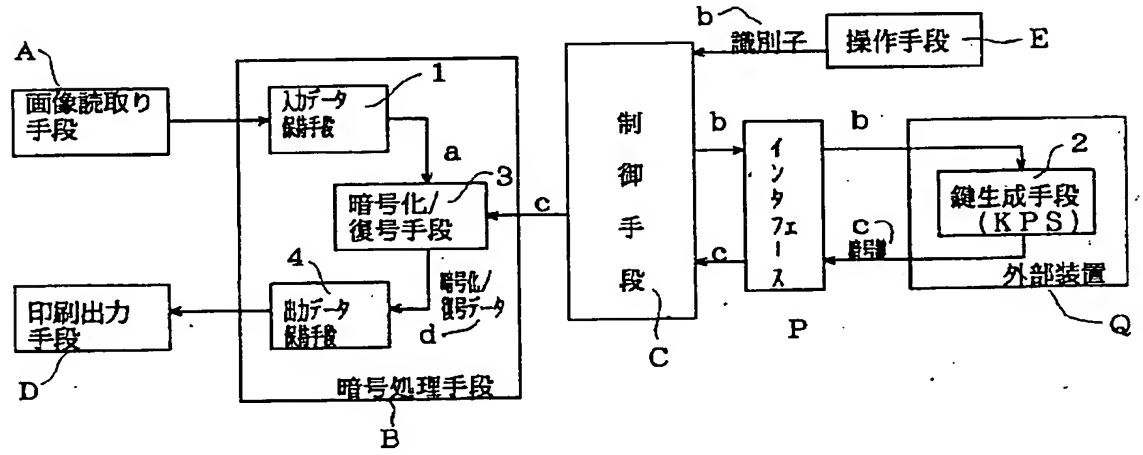
【図２】



【図３】


A
画像読取り手段
a
1
入力データ保持手段
a
制御手段
b
識別子
操作手段
E
b
a
インタフェース
P
b
2
鍵生成手段（KPS）
3
暗号化/復号手段
d
暗号化/復号データ
暗号鍵
c
外部装置
Q
4
出力データ保持手段
d
印刷出力手段
D
C

【図４】


A
画像読取り手段
入力データ保持手段
1
a
暗号化/復号手段
3
c
4
出力データ保持手段
暗号化/復号データ
d
印刷出力手段
D
暗号処理手段
B
制御手段
C
b
識別子
操作手段
E
b
インタフェース
c
P
b
2
鍵生成手段（KPS）
c
暗号鍵
外部装置
Q